BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com
jsmith@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
888 Seventh Avenue
New York, NY 10019
Telephone: (212) 989-9113
Facsimile: (212) 989-9163
E-Mail: scott@bursor.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JEREMY REVITCH, WENDY BURNETT, and GREGORY MAISCH, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

UBER TECHNOLOGIES, INC.,

Defendant.

Case No. 4:17-CV-06835-DMR

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Jeremy Revitch, Wendy Burnett, and Gregory Maisch bring this action on behalf of themselves and all others similarly situated against Uber Technologies, Inc. ("Uber" or "Defendant"). Plaintiffs make the following allegations based upon information and belief, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge.

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to secure and safeguard their personal identifying information ("Private Information"), and that of over 57 million similarly situated people who used its services, and for failing to timely notify Plaintiffs and other class members that hackers stole their Private Information.

2. Uber is one of the world's largest ridesharing companies. It retains Private Information of its users, including names, email and phone information, birthdates, social security numbers, credit card and bank account numbers, and trip information.

3. In October 2016, Uber experienced a data breach in which hackers downloaded the Private Information of 57 million Uber users, including names, email addresses and mobile phone numbers (the "Data Breach"). The hackers also obtained the names and drivers' license numbers of nearly 600,000 Uber drivers in the United States.

4. Uber did not tell its customers or law enforcement what had happened. Instead, Uber paid the hackers a $100,000 ransom in a deal arranged by Uber's chief security officer Joe Sullivan, and under the watch of Uber's former chief executive Travis Kalanik. Uber then conspired with the hackers to hide the Data Breach, which included getting hackers to sign a non-disclosure agreement, and cooking the records to make it appear as if the ransom had been part of a "bug bounty" – a common practice among technology companies in which they pay cyber-security experts (sometimes called "white hat hackers") to attack their software to test for soft spots.

5. It was not until over a year later, on November 21, 2017, that the Data Breach was exposed. That same day, Uber's chief executive Dara Khosrowshahi issued a public statement saying, "You may be asking why we are just talking about this now, a year later. I had the same question. . . . None of this should have happened, and I will not make excuses for it."

PARTIES

6. Plaintiff Jeremy Revitch is, and at all times mentioned herein was, a resident of Mill Valley, California and a citizen of the State of California. Mr. Revitch first used Uber's services as a rider in June 2014. As a result of using Uber's services, Mr. Revitch's Personal Information was stored by Uber and later stolen and put at risk during the Data Breach. The Data Breach and disclosure of the Private Information has immediately, directly and substantially increased Mr. Revitch's risk of identity theft. Indeed, information such as data breach victims' names, birth dates, email addresses, and other identifying information alone creates a material risk of identity theft. As a result of the Data Breach, Mr. Revitch also has suffered a loss of privacy, nuisance and diminished value of Private Information, and must now expend additional time and money mitigating the threat of identity theft that would not be necessary but for the Data Breach.

7. Wendy Burnett resides in Inglewood, California, and has used Uber's services as a driver since approximately January 2016 and as a rider since approximately 2013. As a result of using Uber's services, Ms. Burnett's Personal Information was stored by Uber and later stolen and put at risk during the Data Breach. The Data Breach and disclosure of the Private Information has immediately, directly and substantially increased Ms. Burnett's risk of identity theft. Indeed, information such as data breach victims' names, birth dates, email addresses, and other identifying information alone creates a material risk of identity theft. As a result of the Data Breach, Ms. Burnett also has suffered a loss of privacy, nuisance and diminished value of Private Information, and must now expend additional time and money mitigating the threat of identity theft that would not be necessary but for the Data Breach.

8. Gregory Maisch resides in Hoboken, New Jersey, and has used Uber's services as a rider since approximately 2014. As a result of using Uber's services, Mr. Maisch's Personal Information was stored by Uber and later stolen and put at risk during the Data Breach. The Data Breach and disclosure of the Private Information has immediately, directly and substantially increased Mr. Maisch's risk of identity theft. Indeed, information such as data breach victims' names, birth dates, email addresses, and other identifying information alone creates a material risk of

identity theft. As a result of the Data Breach, Mr. Maisch also has suffered a loss of privacy, nuisance and diminished value of Private Information, and must now expend additional time and money mitigating the threat of identity theft that would not be necessary but for the Data Breach.

9. Uber Technologies, Inc. is a Delaware company with headquarters in San Francisco, California. The company operates in every state in the United States and employs approximately 16,000 people.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1337, as well as jurisdiction over the state law claims pursuant to 28 U.S.C. §§ 1332(d) and 1367 because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which some members of the proposed Classes are citizens of a state different from the Defendants.

11. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 (b), (c), and (d), because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District.

12. This Court has personal jurisdiction because Defendants do business in this District and a substantial part of the events and injury giving rise to Plaintiffs' claims occurred in this District.

FACTS COMMON TO ALL CLAIMS

A. Uber Colluded with Hackers to Hide a Data Breach Affecting 57 Million of its Customers

13. Uber is the world's largest ride-sharing company, serving customers throughout the United States. Uber provides its services through its mobile software application, which collects users' Private Information when users create, update or use their account. When creating an Uber account, for example, users must provide information such as their name, email, phone number, login name and password, address, credit card or banking information, birth date, and government identification numbers. Uber also tracks when and where riders use its services, and all related

transaction details, as well as information about users' mobile phone device. Uber also collects information about its drivers, such as vehicle, insurance and license information.

14. On November 21, 2017, news broke that Uber had not only suffered a significant data breach in October 2016, but also had engaged in a year-long cover up to hide that fact. The Data Breach affected approximately 57 million users and drivers, and the Personal Information included—at least—the names, email addresses and phone numbers of those people. In addition, the hackers obtained the driver's license numbers for approximately 600,000 drivers in the United States.

15. Uber disclosed the breach on its website with a statement by its CEO Dara Khosrowshahi.

16. In that statement, Mr. Khosrowshahi disclosed that "two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use." He further explained, "the individuals were able to download files containing a significant amount of . . . information, including: The names and driver's license numbers of around 600,000 drivers in the United States . . . and [s]ome personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers."

17. Recognizing the imminent and direct threat of injury caused by the Data Breach, Uber stated, "We encourage all our users to regularly monitor their credit and accounts, including their Uber account, for any issues," and to contact the company "if you see anything unexpected or

unusual related to your Uber account."[1]

18. In his statement, Mr. Khosrowshahi went on to say, "You may be asking why we are just talking about this now, a year later. I had the same question." Yet he provided no answer in his public statement. Instead, Mr. Khosrowshahi conceded, "None of this should have happened, and I will not make excuses for it."

19. Mr. Khosrowshahi also failed to disclose in his statement that Uber had conspired with the hackers for over a year to hide the Data Breach from Uber customers and law enforcement officials. When the hackers demanded $100,000, Uber acquiesced to the demand on condition that the hackers sign a non-disclosure agreement. To further conceal what happened, Uber made it appear as if the payout had been part of a "bug bounty" – a common practice among technology companies in which they pay cyber-security experts (sometimes called "white hat hackers") to attack their software to test for soft spots.

20. Uber's chief security officer at the time, Joe Sullivan, and Uber's chief executive at the time, Travis Kalanick, arranged the deal with the hackers. Uber has fired Mr. Sullivan, along with Craig Clark, the company's legal director of security and law enforcement. Mr. Kalanick is no longer Uber's chief executive, although he remains on Uber's board.

21. Security experts and law enforcement officials have repeatedly warned companies against paying hackers a ransom to cover up breaches or return stolen data. In a 2016, for example, the Federal Bureau of Investigation ("FBI") warned, "Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."[2]

---

[1] Information about 2016 Data Security Incident, *available at* https://help.uber.com/h/12c1e9d1-4042-4231-a3ec-3605779b8815

[2] Incidents of Ransomware on the Rise, *available at* https://www.fbi.gov/news/ stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

B. Uber Has a History of Betraying its Users' Trust in Safeguarding Their Private Information

22. In its Privacy Policy, Uber repeatedly urges its users to trust and rely on Uber to safeguard their Private Information with statements like:

- "When you use Uber, you trust us with your information. We are committed to keeping that trust."
- "We care about you & the trust you give us."
- "We work around the clock to protect your data from fraud, abuse, and unauthorized access."

23. Uber further promises its users: "We take the security of your data seriously. Uber uses technical safeguards like encryption, authentication, fraud detection, and secure software development to protect your information. We also have an extensive team of data security and privacy experts working around the clock to prevent theft, fraud, or abuse of your information."

24. The reality, however, is that Uber has a pattern of showing contempt for Private Information and hiding data breaches from its users and government agencies. At the time of the Data Breach, Uber was already embroiled in litigation with government agencies in the United States over an earlier data breach that Uber failed to promptly disclose to its users. In August 2017, Uber negotiated a settlement with the Federal Trade Commission ("FTC") over its handling of consumer data and other, unrelated security missteps. However, Uber did not disclose last year's Data Breach to the FTC, prompting some U.S. lawmakers to urge the FTC to back out of the settlement and seek higher penalties.

CLASS ACTION ALLEGATIONS

25. Plaintiffs seek relief in his individual capacity and as a representative of all others who are similarly situated. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of a Nationwide Class and/or California subclass.

26. The Nationwide Class is defined as all persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016 (the "National Class").

27. The California Class is defined as all persons residing in California whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016 (the "California Class").

28. Excluded from the Classes are Defendant; any of its corporate affiliates; any of their directors, officers, or employees; any persons who timely elects to be excluded from any of the Classes; any government entities; and any judge to whom this case is assigned and their immediate family and court staff.

29. The members of each Class are so numerous that the joinder of all members is impractical. Based on Defendant's statements about the scope of the Data Breach, each Class likely includes millions of people.

30. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual class members. These common questions of law and fact include, without limitation:

a. Whether Defendant violated California Civil Code § 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether Defendant violated California Civil Code § 1798.82 by failing to promptly notify class members their Private Information had been compromised;

c. Whether Defendant violated California Business and Professions Code § 17200, *et seq.*;

d. Whether Uber had a legal duty to use reasonable security measures to protect Private Information;

e. The nature of the relief, including equitable relief and damages, to which Plaintiffs and the class members are entitled.

31. Plaintiffs' claims are typical of the claims of the members of the Classes, and Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs and all members of the Classes are similarly affected by Uber's wrongful conduct in that their Private Information has been exposed without their authorization.

32. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes.

33. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Classes.

34. Plaintiffs are represented by counsel competent and experienced in the prosecution of consumer protection and tort litigation.

35. The questions of law and fact common to the members of the Classes predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

36. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense if numerous individual actions. The benefits of proceeding as a class, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any potential difficulties in managing this class action.

COUNT I

Violation of California's Civil Code §§ 1789.81.5, 1798.82, 1798.83

37. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

38. California Civil Code § 1798.81.5 requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

39. The Private Information at issue here is "Personal information" within the meaning of Civil Code § 1798.80.

40. Plaintiffs and other Class members qualify as "Customer[s]" as defined in Civil

Code § 1798.80, because they provided their personal information to Defendant in order to use Uber's services.

41. Defendant violated Civil Code § 1798.81.5 by failing to maintain reasonable security procedures and practices, resulting in the compromise of Private Information in the Data Breach.

42. Defendant violated Civil Code §§ 1798.82 and 1798.83 by failing to promptly notify all people affected by the Data Breach that their Private Information had been acquired by an unauthorized person, or was reasonably believed to have been acquired by an unauthorized person.

43. As a result of Defendants' violations described here, Plaintiffs and class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in this Complaint.

44. Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82 were willful, intentional or, at a minimum, reckless.

45. Plaintiffs seek, on behalf of themselves and class members, all relief permitted under Civil Code § 1798.84, including damages, statutory penalties, injunctive relief, and attorney's fees and costs.

COUNT II

Violation of California's Unfair Competition law, Bus. & Prof. Code § 17200 *et seq*.

46. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

47. Defendant engaged in unfair, fraudulent and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

48. Plaintiffs and class members suffered an injury in fact and lost money or property because of Defendant's alleged violations of the UCL.

49. The acts, omissions, and conduct of Defendant as alleged constitute a "business practice" within the meaning of the UCL.

50. Defendant violated the unlawful prong of the UCL by violating Civil Code Sections 1798.81.5 and 1798.82, as alleged above.

51. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because they offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and other class members. The harm cause by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

52. Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer by misrepresenting in its Privacy Policy that it had adequate measures to prevent data theft, and by failing to disclose that it does not adhere to industry-standard security practices. A reasonable person would find Defendants' misrepresentations and omissions material when deciding whether to agree to use Uber's services and provide Uber with Private Information.

53. As a result of Defendant's violations of the UCL, Plaintiffs and class members are entitled to injunctive relief and restitution of all funds Defendant acquired as a result of its unfair competition, including fees that Defendant retained for rides given or taken by Plaintiffs and other class members.

COUNT III

Negligence / Negligence Per Se

54. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

55. Defendant owed a duty to Plaintiffs and class members, who were required to provide their Private Information to Defendant in order to use its services. Defendant created a duty through its voluntary actions in collecting and storing the Private Information for its own benefit, as well as by its assurances (in its Privacy Policy and elsewhere) that it would safeguard that information.

56. Defendant's duty required it, among other things, to design and employ cybersecurity systems, anti-hacking technologies, and intrusion detection and reporting systems sufficient to protect Private Information from unauthorized access and to promptly alert its users of data breaches.

57. Defendant also had a duty to delete any Private Information that was no longer needed to serve its drivers' and riders' needs, and not use former drivers' or riders' Private Information in the conduct of its business going forward.

58. Defendant breached its duties by, among other things: failing to maintain appropriate technological and other systems to prevent unauthorized access; failing to minimize the Private Information that any intrusion could compromise; failing to detect the Data Breach in a timely manner; failing to promptly notify Plaintiffs and class members of the Data Breach.

59. Defendants' breaches of its duties provided the means for third parties to access, obtain, and misuse the Private Information of Plaintiffs and the class members without authorization. It was reasonably foreseeable that such breaches would expose the Private Information to criminals and other unauthorized access.

60. But for Defendant's breach of its duties, class members' Private Information would not have been compromised in the Data Breach.

61. As a result of Defendant's negligence, Plaintiffs and class member suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and class member must more closely monitor their financial accounts and credit histories to guard against identity theft and misuse of their Private Information. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized release of Plaintiffs' and class member' Private Information also diminished the value of that Private Information.

62. Defendant's violations of California's Civil Code §§ 1789.81.5, 1798.82, 1798.83, are negligence *per se*.

63. The damages to Plaintiffs and other class members were a proximate, reasonably foreseeable result of Defendant's breaches of its duties. Plaintiffs and class member are entitled to damages in an amount to be proven at trial.

COUNT IV

Unjust enrichment

64. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

65. Defendant knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and class members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and class members by utilizing cheaper, ineffective security measures. Plaintiffs and class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security.

66. Plaintiffs and class members suffered and will continue to suffer injuries in the form of identity theft, attempted identity theft, the expense in mitigating harms, diminished value of Private Information, loss of privacy, and nuisance.

67. Plaintiffs, on behalf of themselves and the class members, therefore seek relief in the form of restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment on behalf of themselves and members of the classes as follows:

A. For an order certifying the Nationwide Class and/or California Subclass under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiffs as Class and Subclass representatives; and naming Plaintiffs' attorneys as Class Counsel representing the Class and Subclass members;

B. For an order finding in favor of Plaintiffs, the nationwide Class, and California Subclass on all counts asserted herein;

C. For an order awarding compensatory damages, statutory damages and/or restitution in amounts to be determined by the Court and/or jury;

D. For injunctive relief enjoining the illegals acts detailed herein;

E. For prejudgment interest on all amounts awarded;

F. For an order awarding Plaintiffs their reasonable attorneys' fees and expenses and costs of suit;

G. Such other or further relief as the Court may deem appropriate.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: February 15, 2018

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Joel D. Smith*
Joel D. Smith

L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com
jsmith@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
888 Seventh Avenue
New York, NY 10019
Telephone: (212) 989-9113
Facsimile: (212) 989-9163
E-Mail: scott@bursor.com

Counsel for Plaintiffs